

FILED
LODGEDENTERED
RECEIVED

FEB -1 2016

UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Seattle, WA

Case No.

MT/6-38

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The residence at [REDACTED] Seattle, WA [REDACTED] as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § (2252 (a)(2)	Receipt and Distribution of Child Pornography and
Title 18, U.S.C. § (2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

DEPUTY CLERK
 ATTEST: WILLIAM M. MCCOOL
 Clerk, U.S. District Court
 Western District of Washington
 Deputy Clerk

Applicant's signature

Ingrid Arbuthnot-Stohl, Special Agent FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 2-1-16

Judge's signature

City and state: Seattle, WASHINGTON

Mary Alice Theiller, U.S. MAGISTRATE JUDGE

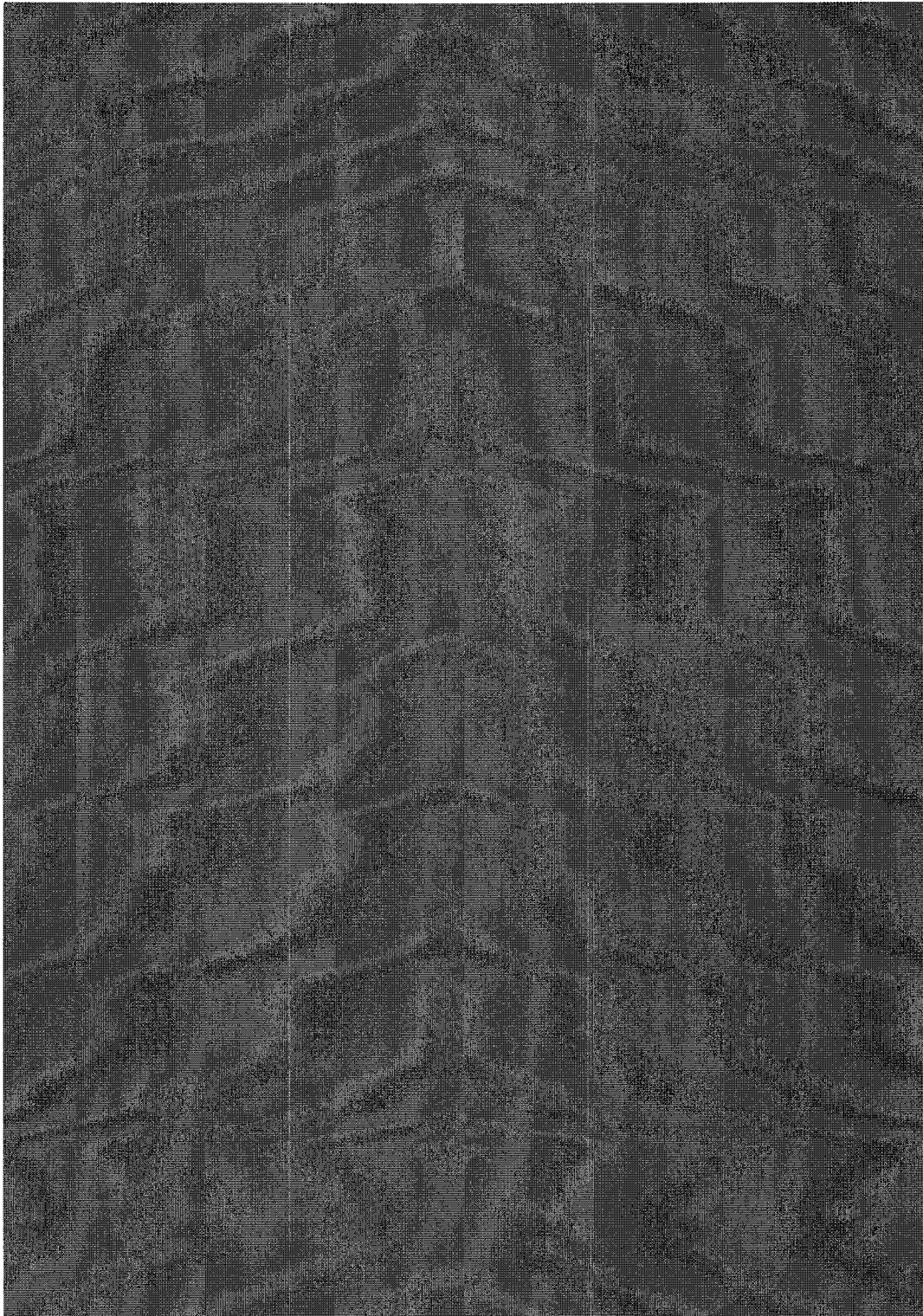
Printed name and title

ATTACHMENT A**DESCRIPTION OF LOCATION TO BE SEARCHED**

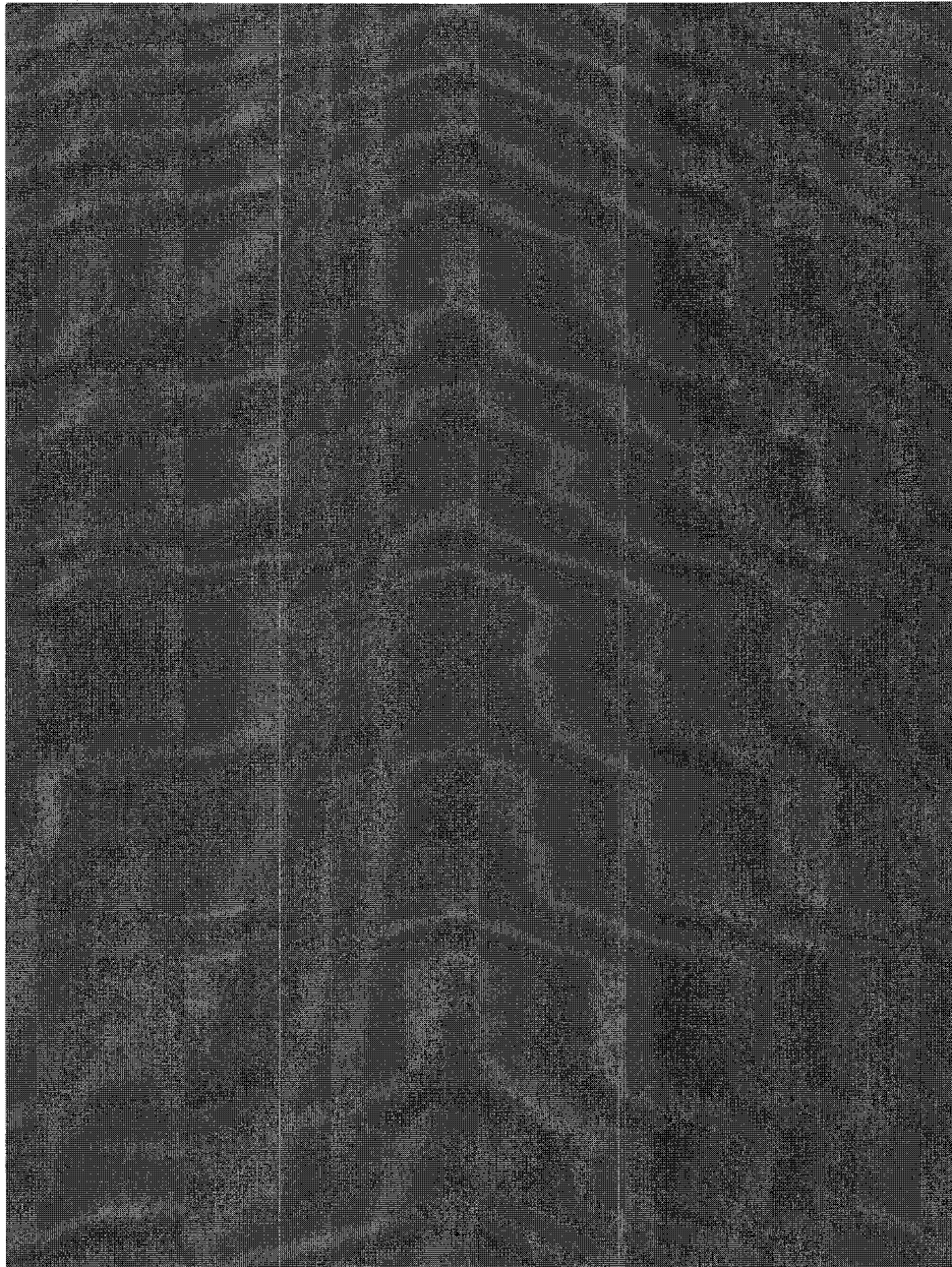
1. The location known as [REDACTED] **Seattle, WA** [REDACTED] is identified as follows: The location is a multi-story apartment building. The front entrance faces [REDACTED] and has glass doors with a silver-colored frame. The numbers [REDACTED] are stenciled above the door. There is a set of interior doors that lead to an entry way and elevator. [REDACTED] is located on the [REDACTED] on the [REDACTED] side of the building. The apartment door is cream colored with the numbers [REDACTED] affixed on the wall next to the door.

The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES of [REDACTED] **Seattle, WA** [REDACTED], and any storage units/outbuildings.

PICTURE



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



ATTACHMENT B**Information to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251 and 2252:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
 4. Child pornography and child erotica.
 5. Records, information, and items relating to violations of the statutes described above including
 - a. Records, information, and items relating to the occupancy or ownership of [REDACTED] Seattle, WA [REDACTED] including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

- 1 c. Records and information relating to sexual exploitation of children,
2 including correspondence and communications between users of Website
3 A.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON

ss

COUNTY OF KING

I, Ingrid Arbuthnot-Stohl, being first duly sworn on oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since December 2010. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in numerous forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2251(d) and (e) (advertising, attempting to advertise, and conspiracy to advertise child pornography); 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of pornography), are located [REDACTED] [REDACTED] Seattle, WA [REDACTED] (hereinafter the "SUBJECT PREMISES"). I

submit this application and affidavit in support of a search warrant authorizing a search of

Affidavit in Support of Application For Search Warrant- 1

2016R00054

1 the SUBJECT PREMISES, as further described in Attachments A and B, incorporated
 2 herein by reference, which is located in the Western District of Washington. Located
 3 within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and
 4 instrumentalities of the foregoing criminal violations. I request authority to search the
 5 entire SUBJECT PREMISES, including the residential dwelling and any computer and
 6 computer media located therein where the items specified in Attachment B may be found,
 7 and to seize all items listed in Attachment B as contraband and instrumentalities, fruits,
 8 and evidence of crime.

9 3. The statements contained in this affidavit are based in part on: information
 10 provided by FBI Special Agents; written reports about this and other investigations that I
 11 have received, directly or indirectly, from other law enforcement agents, information
 12 gathered from the service of administrative subpoenas; the results of physical and
 13 electronic surveillance conducted by law enforcement agents; independent investigation
 14 and analysis by FBI agents/analysts and computer forensic professionals; and my
 15 experience, training and background as a Special Agent (SA) with the FBI. Because this
 16 affidavit is being submitted for the limited purpose of securing authorization for the
 17 requested search warrant, I have not included each and every fact known to me
 18 concerning this investigation. Instead, I have set forth only the facts that I believe are
 19 necessary to establish the necessary foundation for the requested warrant.

20 DEFINITIONS

21 4. The following definitions apply to this Affidavit and attachments hereto:

- 22 a. "Bulletin Board" means an Internet-based website that is either secured
 23 (accessible with a password) or unsecured, and provides members with the
 24 ability to view postings by other members and make postings themselves.
 25 Postings can contain text messages, still images, video images, or web
 26 addresses that direct other members to specific content the poster wishes.
 27 Bulletin boards are also referred to as "internet forums" or "message boards."
 28 A "post" or "posting" is a single message posted by a user. Users of a bulletin

board may post messages in reply to a post. A message "thread," often labeled

1 a "topic," refers to a linked series of posts and reply messages. Message
2 threads or topics often contain a title, which is generally selected by the user
3 who posted the first message of the thread. Bulletin boards often also provide
4 the ability for members to communicate on a one-to-one basis through
5 "private messages." Private messages are similar to e-mail messages that are
6 sent between two members of a bulletin board. They are accessible only by the
7 user who sent/received such a message, or by the Website Administrator.

8 b. "Chat" refers to any kind of communication over the Internet that offers a real-
9 time transmission of text messages from sender to receiver. Chat messages are
10 generally short in order to enable other participants to respond quickly and in a
11 format that resembles an oral conversation. This feature distinguishes chatting
12 from other text-based online communications such as Internet forums and
13 email.

14 c. "Child Erotica," as used herein, means materials or items that are sexually
15 arousing to persons having a sexual interest in minors but that are not, in and of
16 themselves, legally obscene or that do not necessarily depict minors in sexually
17 explicit conduct.

18 d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any
19 visual depiction of sexually explicit conduct where (a) the production of the
20 visual depiction involved the use of a minor engaged in sexually explicit
21 conduct, (b) the visual depiction is a digital image, computer image, or
22 computer-generated image that is, or is indistinguishable from, that of a minor
23 engaged in sexually explicit conduct, or (c) the visual depiction has been
24 created, adapted, or modified to appear that an identifiable minor is engaged in
25 sexually explicit conduct.

26 e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as
27 "an electronic, magnetic, optical, electrochemical, or other high speed data
28 processing device performing logical or storage functions, and includes any

1 data storage facility or communications facility directly related to or operating
2 in conjunction with such device.”

3 f. “Computer Server” or “Server,” as used herein, is a computer that is attached
4 to a dedicated network and serves many users. A web server, for example, is a
5 computer which hosts the data associated with a website. That web server
6 receives requests from a user and delivers information from the server to the
7 user’s computer via the Internet. A domain name system (“DNS”) server, in
8 essence, is a computer on the Internet that routes communications when a user
9 types a domain name, such as www.cnn.com, into his or her web browser.

10 Essentially, the domain name must be translated into an Internet Protocol
11 (“IP”) address so the computer hosting the web site may be located, and the
12 DNS server provides this function.

13 g. “Computer hardware,” as used herein, consists of all equipment which can
14 receive, capture, collect, analyze, create, display, convert, store, conceal, or
15 transmit electronic, magnetic, or similar computer impulses or data. Computer
16 hardware includes any data-processing devices (including, but not limited to,
17 central processing units, internal and peripheral storage devices such as fixed
18 disks, external hard drives, floppy disk drives and diskettes, and other memory
19 storage devices); peripheral input/output devices (including, but not limited to,
20 keyboards, printers, video display monitors, and related communications
21 devices such as cables and connections), as well as any devices, mechanisms,
22 or parts that can be used to restrict access to computer hardware (including, but
23 not limited to, physical keys and locks).

24 h. “Computer software,” as used herein, is digital information which can be
25 interpreted by a computer and any of its related components to direct the way
26 they work. Computer software is stored in electronic, magnetic, or other
27 digital form. It commonly includes programs to run operating systems,
28 applications, and utilities.

i. “Computer-related documentation,” as used herein, consists of written,

1
2 recorded, printed, or electronically stored material which explains or illustrates
3 how to configure or use computer hardware, computer software, or other
4 related items.

5 j. "Computer passwords, pass-phrases and data security devices," as used herein,
6 consist of information or items designed to restrict access to or hide computer
7 software, documentation, or data. Data security devices may consist of
8 hardware, software, or other programming code. A password or pass-phrase (a
9 string of alpha-numeric characters) usually operates as a sort of digital key to
10 "unlock" particular data security devices. Data security hardware may include
11 encryption devices, chips, and circuit boards. Data security software of digital
12 code may include programming code that creates "test" keys or "hot" keys,
13 which perform certain pre-set security functions when touched. Data security
14 software or code may also encrypt, compress, hide, or "booby-trap" protected
15 data to make it inaccessible or unusable, as well as reverse the process to
16 restore it.

17 k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network
18 protocol used to transfer computer files from one host to another over a
19 computer network, such as the Internet. FTP is built on client-server
20 architecture and uses separate control and data connections between the client
21 and the server.

22 l. "Host Name." A Host Name is a name assigned to a device connected to a
23 computer network that is used to identify the device in various forms of
24 electronic communication, such as communications over the Internet;

25 m. "Hyperlink" refers to an item on a web page which, when selected, transfers
26 the user directly to another location in a hypertext document or to some other
27 web page.

28 n. The "Internet" is a global network of computers and other electronic devices
that communicate with each other. Due to the structure of the Internet,

1 connections between devices on the Internet often cross state and international
2 borders, even when the devices communicating with each other are in the same
3 state.

4 o. "Internet Service Providers" ("ISPs"), as used herein, are commercial
5 organizations that are in business to provide individuals and businesses access
6 to the Internet. ISPs provide a range of functions for their customers including
7 access to the Internet, web hosting, e-mail, remote storage, and co-location of
8 computers and other communications equipment. ISPs can offer a range of
9 options in providing access to the Internet including telephone based dial-up,
10 broadband based access via digital subscriber line ("DSL") or cable television,
11 dedicated circuits, or satellite based subscription. ISPs typically charge a fee
12 based upon the type of connection and volume of data, called bandwidth,
13 which the connection supports. Many ISPs assign each subscriber an account
14 name – a user name or screen name, an "e-mail address," an e-mail mailbox,
15 and a personal password selected by the subscriber. By using a computer
16 equipped with a modem, the subscriber can establish communication with an
17 Internet Service Provider ("ISP") over a telephone line, through a cable system
18 or via satellite, and can access the Internet by using his or her account name
19 and personal password.

20 p. "Internet Protocol address" or "IP address" refers to a unique number used by a
21 computer to access the Internet. IP addresses can be "dynamic," meaning that
22 the ISP assigns a different unique number to a computer every time it accesses
23 the Internet. IP addresses might also be "static," if an ISP assigns a user's
24 computer a particular IP address which is used each time the computer
25 accesses the Internet. IP addresses are also used by computer servers,
26 including web servers, to communicate with other computers.

27 q. Media Access Control ("MAC") address. The equipment that connects a
28 computer to a network is commonly referred to as a network adapter.

1 Most network adapters have a MAC address assigned by the manufacturer of
2 the adapter that is designed to be a unique identifying number. A unique MAC
3 address allows for proper routing of communications on a network. Because
4 the MAC address does not change and is intended to be unique, a MAC
5 address can allow law enforcement to identify whether communications sent or
6 received at different times are associated with the same adapter.

7 r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. §
8 2256(1).

9 s. The terms "records," "documents," and "materials," as used herein, include all
10 information recorded in any form, visual or aural, and by any means, whether
11 in handmade form (including, but not limited to, writings, drawings, painting),
12 photographic form (including, but not limited to, microfilm, microfiche, prints,
13 slides, negatives, videotapes, motion pictures, photocopies), mechanical form
14 (including, but not limited to, phonograph records, printing, typing) or
15 electrical, electronic or magnetic form (including, but not limited to, tape
16 recordings, cassettes, compact discs, electronic or magnetic storage devices
17 such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"),
18 Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory
19 sticks, optical disks, printer buffers, smart cards, memory calculators,
20 electronic dialers, or electronic notebooks, as well as digital data files and
21 printouts or readouts from any magnetic, electrical or electronic storage
22 device).

23 t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a
24 remote server. SSH provides an encrypted session for transferring files and
25 executing server programs.

26 u. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse,
27 including genital-genital, oral-genital, or oral-anal, whether between persons of
28 the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or

1 masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of
2 any person. See 18 U.S.C. § 2256(2).

3 v. "URL" is an abbreviation for Uniform Resource Locator and is another name
4 for a web address. URLs are made of letters, numbers, and other symbols in a
5 standard form. People use them on computers by clicking a pre-prepared link
6 or typing or copying and pasting one into a web browser to make the computer
7 fetch and show some specific resource (usually a web page) from another
8 computer (web server) on the Internet.

9 w. "Visual depictions" include undeveloped film and videotape, and data stored
10 on computer disk or by electronic means, which is capable of conversion into a
11 visual image. See 18 U.S.C. § 2256(5).

12 x. "Website" consists of textual pages of information and associated graphic
13 images. The textual information is stored in a specific format known as Hyper-
14 Text Mark-up Language ("HTML") and is transmitted from web servers to
15 various web clients via Hyper-Text Transport Protocol ("HTTP");

16 **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

17 5. [REDACTED] or a user of the Internet account at [REDACTED]
18 [REDACTED] Seattle, WA [REDACTED] has been linked to an online community of individuals who
19 regularly send and receive child pornography via a website that operated on an
20 anonymous online network. The website is described below and referred to herein as
21 "Website A."¹ There is probable cause to believe that [REDACTED] or a user of the
22 Internet account at [REDACTED] Seattle, WA [REDACTED] knowingly accessed,
23 viewed, and received child pornography on "Website A."

24
25
26 1 The actual name of "Website A" is known to law enforcement. Disclosure of the name of the site would
27 potentially alert its members to the fact that law enforcement action is being taken against the site and its users,
28 potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence.
Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter,
specific names and other identifying factors have been replaced with generic terms and the website will be identified
as "Website A."

The Network²

6. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

7. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to

² The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

³ Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

1 "Website A." Rather, a user had to have obtained the web address for "Website A"
2 directly from another source, such as other users of "Website A," or from online postings
3 describing both the sort of content available on "Website A" and its location. Accessing
4 "Website A" therefore required numerous affirmative steps by the user, making it
5 extremely unlikely that any user could have simply stumbled upon "Website A" without
6 first understanding its content and knowing that its primary purpose was to advertise and
7 distribute child pornography.

8 8. The Network's software protects users' privacy online by bouncing their
9 communications around a distributed network of relay computers run by volunteers all
10 around the world, thereby masking the user's actual IP address which could otherwise be
11 used to identify a user.

12 9. The Network also makes it possible for users to hide their locations while
13 offering various kinds of services, such as web publishing, forum/website hosting, or an
14 instant messaging server. Within the Network itself, entire websites can be set up which
15 operate the same as regular public websites with one critical exception - the IP address
16 for the web server is hidden and instead is replaced with a Network-based web address.
17 A user can only reach such sites if the user is using the Network client and operating in
18 the Network. Because neither a user nor law enforcement can identify the actual IP
19 address of the web server, it is not possible to determine through public lookups where
20 the computer that hosts the website is located. Accordingly, it is not possible to obtain
21 data detailing the activities of the users from the website server through public lookups.

22 **Description of "Website A" and its Content**

23 10. "Website A" was a child pornography bulletin board and website dedicated
24 to the advertisement and distribution of child pornography and the discussion of matters
25 pertinent to the sexual abuse of children, including the safety and security of individuals
26 who seek to sexually exploit children online. On or about February 20, 2015, the
27 computer server hosting "Website A" was seized from a web-hosting facility in Lenoir,
28 North Carolina. The website operated in Newington, Virginia, from February 20, 2015,

1 until March 4, 2015, at which time "Website A" ceased to operate. Between February
2 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the
3 United States District Court for the Eastern District of Virginia monitored electronic
4 communications of users of "Website A." Before, during, and after its seizure by law
5 enforcement, law enforcement agents viewed, examined and documented the contents of
6 "Website A," which are described below.

7 11. According to statistics posted on the site, "Website A" contained a total of
8 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The
9 website appeared to have been operating since approximately August 2014, which is
10 when the first post was made on the message board. Between September of 2014 and
11 February 19, 2015, on the main page of the site, located to either side of the site name
12 were two images depicting partially clothed prepubescent girls with their legs spread
13 apart, along with the text underneath stating, "No cross-board reposts, .7z preferred,
14 encrypt filenames, include preview, Peace out."⁵ Based on my training and experience,
15 I know that: "no cross-board reposts" refers to a prohibition against material that is
16 posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a
17 preferred method of compressing large files or sets of files for distribution. Two data-
18 entry fields with a corresponding "Login" button were located to the right of the site
19 name. Located below the aforementioned items was the message, "Warning! Only
20 registered members are allowed to access the section. Please login below or 'register an
21 account' [(a hyperlink to the registration page)] with "[Website A]." Below this message
22 was the "Login" section, consisting of four data-entry fields with the corresponding text,
23 "Username, Password, Minutes to stay logged in, and Always stay logged in."

24 12. Upon accessing the "register an account" hyperlink, there was a message
25 that informed users that the forum required new users to enter an email address that looks
26 to be valid. However, the message instructed members not to enter a real email address.

27
28 ⁵ On February 19, 2015, the site administrator replaced those two images with a single image, located to the left of
the site name, depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a
chair with her legs crossed, in a sexually suggestive manner, and the text "No cross-board reposts, .7z preferred,
Encrypt filenames, Include preview," to the right of the image.

1 The message further stated that once a user registered (by selecting a user name and
2 password), the user would be able to fill out a detailed profile. The message went on to
3 warn the user “[F]or your security you should not post information here that can be used
4 to identify you.” The message further detailed rules for the forum and provided other
5 recommendations on how to hide the user’s identity for the user’s own security.

6 13. After accepting the above terms, registration to the message board then
7 required a user to enter a username, password, and e-mail account; although a valid e-
8 mail account was not required as described above.

9 14. After successfully registering and logging into the site, the user could
10 access any number of sections, forums, and sub-forums. Some of the sections, forums,
11 and sub-forums available to users included: (a) How to; (b) General Discussion; (c)
12 [Website A] information and rules; and (d) Security & Technology discussion. Additional
13 sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c)
14 Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos –
15 Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and
16 experience, I know that “jailbait” refers to underage but post-pubescent minors; the
17 abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit
18 conduct); and “scat” refers to the use of feces in various sexual acts, watching someone
19 defecating, or simply seeing the feces. An additional section and forum was also listed
20 in which members could exchange usernames on a Network-based instant messaging
21 service that I know, based upon my training and experience, to be commonly used by
22 subjects engaged in the online sexual exploitation of children.

23 15. A review of the various topics within the above forums revealed each topic
24 contained a title, the author, the number of replies, the number of views, and the last post.
25 The “last post” section of a particular topic included the date and time of the most recent
26 posting to that thread as well as the author. Upon accessing a topic, the original post
27 appeared at the top of the page, with any corresponding replies to the original post
28 included in the post thread below it. Typical posts appeared to contain text, images,

thumbnail-sized previews of images, compressed files (such as Roshal Archive files,
Affidavit in Support of Application For Search Warrant- 12

2016R00054

1 commonly referred to as “.rar” files, which are used to store and distribute multiple files
2 within a single file), links to external sites, or replies to previous posts.

3 16. A review of the various topics within the “[Website A] information and
4 rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums
5 revealed that the majority contained general information in regards to the site,
6 instructions and rules for how to post, and welcome messages between users.

7 17. A review of topics within the remaining forums revealed the majority
8 contained discussions about, and numerous images that appeared to depict, child
9 pornography and child erotica depicting prepubescent girls, boys, and toddlers.

10 Examples of these are as follows:

11 (a) On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum
12 “Pre-teen – Videos - Girls HC” that contained numerous images depicting
13 child pornography of a prepubescent or early pubescent girl. One of these
14 images depicted the girl being orally penetrated by the penis of a naked male;

15 (b) On January 30, 2015, a user posted a topic entitled “Sammy” in the forum
16 “Pre-teen – Photos – Girls” that contained hundreds of images depicting child
17 pornography of a prepubescent girl. One of these images depicted the female
18 being orally penetrated by the penis of a male; and

19 (c) On September 16, 2014, a user posted a topic entitled “9yo Niece -
20 Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four
21 images depicting child pornography of a prepubescent girl and a hyperlink to
22 an external website that contained a video file depicting what appeared to be
23 the same prepubescent girl. Among other things, the video depicted the
24 prepubescent female, who was naked from the waist down with her vagina and
25 anus exposed, lying or sitting on top of a naked adult male, whose penis was
26 penetrating her anus.

27 18. A list of members, which was accessible after registering for an account,
28 revealed that approximately 100 users made at least 100 posts to one or more of the

forums. Approximately 31 of these users made at least 300 posts. In total, “Website A”

1 contained thousands of postings and messages containing child pornography images.
2 Those images included depictions of nude prepubescent minors lasciviously exposing
3 their genitals or engaged in sexually explicit conduct with adults or other children.

4 19. "Website A" also included a feature referred to as "[Website A] Image
5 Hosting." This feature of "Website A" allowed users of "Website A" to upload links to
6 images of child pornography that are accessible to all registered users of "Website A."
7 On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita"
8 which was created by a particular "Website A" user. The post contained links to images
9 stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in
10 various stages of undress. Some images were focused on the nude genitals of a
11 prepubescent girl. Some images depicted an adult male's penis partially penetrating the
12 vagina of a prepubescent girl.

13 20. Text sections of "Website A" provided forums for discussion of methods
14 and tactics to use to perpetrate child sexual abuse.

- 15 a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the
16 forum "Stories - Non-Fiction" that contained a detailed accounting of an
17 alleged encounter between the user and a 5 year old girl. The user wrote
18 "...it felt amazing feeling her hand touch my dick even if it was through
19 blankets and my pajama bottoms..." The user ended his post with the
20 question, "should I try to proceed?" and further stated that the girl "seemed
21 really interested and was smiling a lot when she felt my cock." A different
22 user replied to the post and stated, "...let her see the bulge or even let her
23 feel you up...you don't know how she might react, at this stage it has to be
24 very playful..."

25 **Court Authorized Use of Network Investigative Technique**

26 21. Websites generally have Internet Protocol ("IP") address logs that can be
27 used to locate and identify the site's users. In such cases, after the seizure of a website
28 whose users were engaging in unlawful activity, law enforcement could review those
logs in order to determine the IP addresses used by users of "Website A" to access the

1 site. A publicly available lookup could then be performed to determine what Internet
2 Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to
3 that ISP to determine the user to which the IP address was assigned at a given date and
4 time.

5 22. However, because of the Network software utilized by "Website A," any
6 such logs of user activity would contain only the IP addresses of the last computer
7 through which the communications of "Website A" users were routed before the
8 communications reached their destinations. The last computer is not the actual user who
9 sent the communication or request for information, and it is not possible to trace such
10 communications back through the Network to that actual user. Such IP address logs
11 therefore could not be used to locate and identify users of "Website A."

12 23. Accordingly, on February 20, 2015, the same date "Website A" was seized,
13 the United States District Court for the Eastern District of Virginia authorized a search
14 warrant to allow law enforcement agents to deploy a Network Investigative Technique
15 ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other
16 identifying information of computers used to access "Website A." Pursuant to that
17 authorization, between February 20, 2015, and approximately March 4, 2015, each time
18 any user or administrator logged into "Website A" by entering a username and password,
19 the FBI was authorized to deploy the NIT which would send one or more
20 communications to the user's computer. Those communications were designed to cause
21 the receiving computer to deliver to a computer known to or controlled by the
22 government data that would help identify the computer, its location, other information
23 about the computer, and the user of the computer accessing "Website A." That data
24 included: the computer's actual IP address, and the date and time that the NIT
25 determined what that IP address was; a unique identifier generated by the NIT (e.g., a
26 series of numbers, letters, and/or special characters) to distinguish the data from that of
27 other computers; the type of operating system running on the computer, including type
28 (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information

1 about whether the NIT had already been delivered to the computer; the computer's Host
2 Name; the computer's active operating system username; and the computer's MAC
3 address.

4 **"jbtoystore" On "Website A"**

5 24. According to data obtained from logs on "Website A," monitoring by law
6 enforcement and the deployment of a NIT, a user with the user name "jbtoystore"
7 engaged in the following activity on "Website A."

8 25. The profile page of user "jbtoystore" indicated this user originally
9 registered an account on "Website A" on December 10, 2014. Profile information on
10 "Website A" may include contact information and other information that is supplied by
11 the user. It also contains information about that user's participation on the site, including
12 statistical information about the user's posts to the site and a categorization of those
13 posts. According to the user "jbtoystore's" profile, this user was a newbie Member of
14 "Website A." Further, according to the Statistics section of this user's profile, the user
15 "jbtoystore" had been actively logged into the website for a total of 2 hours and 35
16 minutes between the dates of December 10, 2014 and February 28, 2015.

17 **IP Address and Identification of User "jbtoystore" on "Website A"**

18 26. According to data obtained from logs on "Website A," monitoring by law
19 enforcement, and the deployment of a NIT, on February 28, 2015, the user "jbtoystore"
20 engaged in the following activity on "Website A" from IP address 104.156.100.205.
21 During the session described below, this user browsed "Website A" after logging into
22 "Website A" with a username and a password.

23 27. On February 28, 2015, the user "jbtoystore" with IP address
24 104.156.100.205 accessed the post entitled "New Tropical Cutie Vid [tc2/2]" which was
25 located in the "Pre-teen Videos", "Girls HC (hardcore)" section of "Website A". Among
26 other things, this post contained links to videos that purported to depict a prepubescent
27 female engaged in hardcore sexual activity.

28 28. On February 28, 2015, the user "jbtoystore" with IP address
104.156.100.205 accessed the post entitled "Brother, sister & Dad All Fucking Each

1 Other (57 minutes, VHC Golden Lolita)" which was located in a section of "Website A"
2 dedicated to Incest themed child pornography. Among other things, this post contained a
3 link to the video and a collection of screenshots that serves as a preview to a video that is
4 available for download. This post preview consisted of 55 embedded images, which I
5 have reviewed, that depicted at least one juvenile female and one juvenile male engaged
6 in various types of penetrative sexual activity with an adult male, including oral and anal
7 sex. The female is a juvenile based upon lack of breast development, lack of pubic hair,
8 lack of hip development, and overall body size. The male is a juvenile based upon his
9 minimal genital development, lack of pubic hair, and overall body size.

10 29. On February 28, 2015, the user "jbtoystore" with IP address
11 104.156.100.205 accessed the post entitled "Cambodia pic dump" which was located in
12 the "Preteen - Girl" section of "Website A". Among other things, this post contained
13 multiple embedded images, which I have reviewed, that depicted one or more
14 prepubescent females engaged in oral and vaginal sexual activity with adult males. One
15 picture is of a juvenile female approximately 10 to 12 years old based upon the lack of
16 hip development, minimal breast development, lack of pubic hair, overall body size, and
17 facial features. The juvenile female is seated on the floor with her hands bound at the
18 wrist and pulled over her head with rope. The juvenile female is sitting with her knees
19 apart to expose her vaginal area. Inserted into the juvenile female's vagina is a pink
20 dildo.

21 30. Using publicly available websites, FBI Special Agents were able to
22 determine that the above IP Address was operated by the Internet Service Provider
23 ("ISP") Wave Broadband.

24 31. In March 2015, an administrative subpoena/summons was served to Wave
25 Broadband requesting information related to the user who was assigned to the above IP
26 address. According to the information received from Wave Broadband, [REDACTED] is
27 receiving Internet service at the address of the SUBJECT PREMISES with an installation
28 date of October 2014. Internet service was current as of April 2015 at the
aforementioned premises.

1 32. Among the information collected by the NIT when it was deployed against
2 "jbtoystore" was the logon name "[REDACTED]", which reflects the middle name of an adult
3 male residing at the SUBJECT PREMISES.

4 33. On November 23, 2015, a search of the CLEAR information database (a
5 public records database that provides names, dates of birth, addresses, associates,
6 telephone numbers, email addresses, etc.) was conducted for [REDACTED]. These public
7 records indicated that [REDACTED] current address is [REDACTED] Seattle, WA
8 [REDACTED] the SUBJECT PREMISES. Also associated with that same address, according to
9 CLEAR, is [REDACTED].

10 34. On or about January 15, 2016, I reviewed the Washington State Department
11 of Motor Vehicles (DMV) database using queries for [REDACTED]. The results yielded
12 information regarding an individual named [REDACTED] currently has a vehicle
13 registered to the SUBJECT PREMISES.

14 35. On or about January 4, 2016, I received information from the United States
15 Postal Service's ("USPS") Delivery Unit that services the SUBJECT PREMISES. USPS
16 personnel indicated that [REDACTED] and [REDACTED] currently receive mail at the
17 SUBJECT PREMISES.

18 36. A check of open source information from the Internet regarding [REDACTED]
19 [REDACTED] in Seattle revealed a LinkedIn account for [REDACTED]. The account included a
20 photo which, when compared to the WA DMV photo, revealed the LinkedIn account as
21 belonging to [REDACTED].

22 **CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH**
23 **INTENT TO VIEW [AND/OR COLLECT, RECEIVE, DISTRIBUTE OR**
24 **ADVERTISE] CHILD PORNOGRAPHY**

25 37. Based on my previous investigative experience related to child
26 pornography investigations, and the training and experience of other law enforcement
27 officers with whom I have had discussions, I know there are certain characteristics
28 common to individuals who utilize web based bulletin boards to access with intent to
view and/or possess, collect, receive images of child pornography:

- a. Individuals who access with intent to view, possess, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals who access with intent to view, possess, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who access with intent to view, possess, and receive child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who access with intent to view, possess, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These

collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to

enable the individual to view the collection, which is valued highly.

- e. Individuals who access with intent to view, possess, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.
- g. Individuals who access with intent to view possess, and receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

38. Based on the following, I believe that a user of the Internet account at SUBJECT PREMISES, likely displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography.

For example:

- a. The user "jbtoystore" logged a total of approximately 2 hours and 35 minutes of total time on Website A between December 10, 2014 and February 28, 2015, and viewed a total of 38 threads on Website A. This demonstrates the user "jbtoystore" purposely accessed and browsed the site for a significant length of time.
- b. The user "jbtoystore" accessed 76 threads that included titles such as "13yo fucked hard", "14yo latin girl having sex with 15yo boy", and "PedoDogs PedoWomen PicturePack". Most of the threads "jbtoystore" accessed contained links to images and/or videos of child pornography.
- c. The user "jbtoystore" chose a username that is consistent with common terms used by those who engage in child pornography. The initials "jb" often refer to "jailbait" which refers to underage males and females.

Background on Computers and Child Pornography

39. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

40. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily

transferred from the camcorder to a computer.

1 41. A device known as a modem allows any computer to connect to another
2 computer through the use of telephone, cable, or wireless connection. Electronic contact
3 can be made to literally millions of computers around the world. The ability to produce
4 child pornography easily, reproduce it inexpensively, and market it anonymously
5 (through electronic communications) has drastically changed the method of distribution
6 and receipt of child pornography. Child pornography can be transferred via electronic
7 mail or through file transfer protocols (FTP) to anyone with access to a computer and
8 modem. Because of the proliferation of commercial services that provide electronic mail
9 service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the
10 computer is a preferred method of distribution and receipt of child pornographic
11 materials.

12 42. The computer's ability to store images in digital form makes the computer
13 itself an ideal repository for child pornography. The size of the electronic storage media
14 (commonly referred to as the hard drive) used in home computers has grown
15 tremendously within the last several years. These drives can store thousands of images at
16 very high resolution. In addition, there are numerous options available for the storage of
17 computer or digital files. One-Terabyte external and internal hard drives are not
18 uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or
19 "flash" drives, which are very small devices which are plugged into a port on the
20 computer. It is extremely easy for an individual to take a photo with a digital camera,
21 upload that photo to a computer, and then copy it (or any other files on the computer) to
22 any one of those media storage devices (CDs and DVDs are unique in that special
23 software must be used to save or "burn" files onto them). Media storage devices can
24 easily be concealed and carried on an individual's person.

25 43. The Internet affords individuals several different venues for obtaining,
26 viewing, and trading child pornography in a relatively secure and anonymous fashion.

27 44. Individuals also use online resources to retrieve and store child
28 pornography, including services offered by Internet Portals such as Yahoo! and Hotmail,

among others. The online services allow a user to set up an account with a remote
Affidavit in Support of Application For Search Warrant- 22

2016R00054

1 computing service that provides e-mail services as well as electronic storage of computer
2 files in any variety of formats. A user can set up an online storage account from any
3 computer with access to the Internet. Even in cases where online storage is used,
4 however, evidence of child pornography can be found on the user's computer or external
5 media in most cases.

6 45. As is the case with most digital technology, communications by way of
7 computer can be saved or stored on the computer used for these purposes. Storing this
8 information can be intentional, i.e., by saving an e-mail as a file on the computer or
9 saving the location of one's favorite websites in, for example, "bookmarked" files.
10 Digital information can also be retained unintentionally, e.g., traces of the path of an
11 electronic communication may be automatically stored in many places (e.g., temporary
12 files or ISP client software, among others). In addition to electronic communications, a
13 computer user's Internet activities generally leave traces or "footprints" in the web cache
14 and history files of the browser used. Such information is often maintained indefinitely
15 until overwritten by other data.

16 **SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

17 46. In addition, based on my training and experience and that of computer
18 forensic agents that I work and collaborate with on a daily basis, I know that in most
19 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
20 electronic evidence stored on a digital device during the physical search of a search site
21 for a number of reasons, including but not limited to the following:

- 22 a. Technical Requirements: Searching digital devices for criminal evidence is
23 a highly technical process requiring specific expertise and a properly
24 controlled environment. The vast array of digital hardware and software
25 available requires even digital experts to specialize in particular systems
26 and applications, so it is difficult to know before a search which expert is
27 qualified to analyze the particular system(s) and electronic evidence found
28 at a search site. As a result, it is not always possible to bring to the search
site all of the necessary personnel,

1 technical manuals, and specialized equipment to conduct a thorough search
2 of every possible digital device/system present. In addition, electronic
3 evidence search protocols are exacting scientific procedures designed to
4 protect the integrity of the evidence and to recover even hidden, erased,
5 compressed, password-protected, or encrypted files. Since ESI is extremely
6 vulnerable to inadvertent or intentional modification or destruction (both
7 from external sources or from destructive code embedded in the system
8 such as a "booby trap"), a controlled environment is often essential to
9 ensure its complete and accurate analysis.

10 b. Volume of Evidence: The volume of data stored on many digital devices is
11 typically so large that it is impossible to search for criminal evidence in a
12 reasonable period of time during the execution of the physical search of a
13 search site. A single megabyte of storage space is the equivalent of 500
14 double-spaced pages of text. A single gigabyte of storage space, or 1,000
15 megabytes, is the equivalent of 500,000 double-spaced pages of text.
16 Computer hard drives are now being sold for personal computers capable of
17 storing up to two terabytes (2,000 gigabytes of data.) Additionally, this
18 data may be stored in a variety of formats or may be encrypted (several new
19 commercially available operating systems provide for automatic encryption
20 of data upon shutdown of the computer).

21 c. Search Techniques: Searching the ESI for the items described in
22 Attachment B may require a range of data analysis techniques. In some
23 cases, it is possible for agents and analysts to conduct carefully targeted
24 searches that can locate evidence without requiring a time-consuming
25 manual search through unrelated materials that may be commingled with
26 criminal evidence. In other cases, however, such techniques may not yield
27 the evidence described in the warrant, and law enforcement personnel with
28 appropriate expertise may need to conduct more extensive searches, such as

1 scanning areas of the disk not allocated to listed files, or peruse every file
2 briefly to determine whether it falls within the scope of the warrant.

3 47. In this particular case, the government anticipates the use of a hash value
4 library to exclude normal operating system files that do not need to be searched, which
5 will facilitate the search for evidence that does come within the items described in
6 Attachment B. Further, the government anticipates the use of hash values and known file
7 filters to assist the digital forensics examiners/agents in identifying known and or
8 suspected child pornography image files. Use of these tools will allow for the quick
9 identification of evidentiary files but also assist in the filtering of normal system files that
10 would have no bearing on the case.

11 48. In accordance with the information in this Affidavit, law enforcement
12 personnel will execute the search of digital devices seized pursuant to this warrant as
13 follows:

14 a. Upon securing the search site, the search team will conduct an initial
15 review of any digital devices/systems to determine whether the ESI contained
16 therein can be searched and/or duplicated on site in a reasonable amount of time
17 and without jeopardizing the ability to accurately preserve the data.

18 b. If, based on their training and experience, and the resources
19 available to them at the search site, the search team determines it is not practical to
20 make an on-site search, or to make an on-site copy of the ESI within a reasonable
21 amount of time and without jeopardizing the ability to accurately preserve the
22 data, then the digital devices will be seized and transported to an appropriate law
23 enforcement laboratory for review and to be forensically copied ("imaged"), as
24 appropriate.

25 c. In order to examine the ESI in a forensically sound manner, law
26 enforcement personnel with appropriate expertise will produce a complete forensic
27 image, if possible and appropriate, of any digital device that is found to contain
28 data or items that fall within the scope of Attachment B of this Affidavit. In

1 addition, appropriately trained personnel may search for and attempt to recover
2 deleted, hidden, or encrypted data to determine whether the data fall within the list
3 of items to be seized pursuant to the warrant. In order to search fully for the items
4 identified in the warrant, law enforcement personnel, which may include
5 investigative agents, may then examine all of the data contained in the forensic
6 image/s and/or on the digital devices to view their precise contents and determine
7 whether the data fall within the list of items to be seized pursuant to the warrant.

8 d. The search techniques that will be used will be only those
9 methodologies, techniques and protocols as may reasonably be expected to find,
10 identify, segregate and/or duplicate the items authorized to be seized pursuant to
11 Attachment B to this Affidavit.

12 e. If, after conducting its examination, law enforcement personnel
13 determine that any digital device is an instrumentality of the criminal offenses
14 referenced above, the government may retain that device during the pendency of
15 the case as necessary to, among other things, preserve the instrumentality evidence
16 for trial, ensure the chain of custody, and litigate the issue of forfeiture.

17 49. In order to search for ESI that falls within the list of items to be seized
18 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
19 search the following items (heretofore and hereinafter referred to as "digital devices"),
20 subject to the procedures set forth above:

21 a. Any digital device capable of being used to commit, further, or store
22 evidence of the offense(s) listed above;

23 b. Any digital device used to facilitate the transmission, creation,
24 display, encoding, or storage of data, including word processing equipment,
25 modems, docking stations, monitors, printers, cameras, encryption devices, and
26 optical scanners;

27 c. Any magnetic, electronic, or optical storage device capable of
28 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or

1 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives,
2 camera memory cards, media cards, electronic notebooks, and personal digital
3 assistants;

4 d. Any documentation, operating logs and reference manuals regarding
5 the operation of the digital device, or software;

6 e. Any applications, utility programs, compilers, interpreters, and other
7 software used to facilitate direct or indirect communication with the device
8 hardware, or ESI to be searched;

9 f. Any physical keys, encryption devices, dongles and similar physical
10 items that are necessary to gain access to the digital device, or ESI; and

11 g. Any passwords, password files, test keys, encryption codes or other
12 information necessary to access the digital device or ESI.

13 **Instrumentalities**

14 50. Based on the information in this Affidavit, I also believe that the digital
15 device(s) at the SUBJECT PREMISES are instrumentalities of crime and constitute the
16 means by which violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child
17 Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) have
18 been committed. Therefore, I believe that in addition to seizing the digital devices to
19 conduct a search of their contents as set forth herein, there is probable cause to seize
20 those digital devices as instrumentalities of criminal activity.

21 //

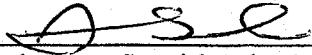
22 //

23 //


24
25
26 **Conclusion**

27 51. Based on the foregoing, there is probable cause to believe that the federal
28 criminal statutes cited herein have been violated, and that the contraband, property,
evidence, fruits and instrumentalities of these offenses, more fully described in

1 Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in
2 Attachment A. I respectfully request that this Court issue a search warrant for the
3 SUBJECT PREMISES, authorizing the seizure and search of the items described in
4 Attachment B.

5
6
7 
8 Special Agent Ingrid Arbuthnot-Stohl
9 Federal Bureau of Investigation

10
11 Sworn to me this 1 day of February 2016.

12
13 
14 MARY ALICE THEILER
15 United States Magistrate Judge
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A**DESCRIPTION OF LOCATION TO BE SEARCHED**

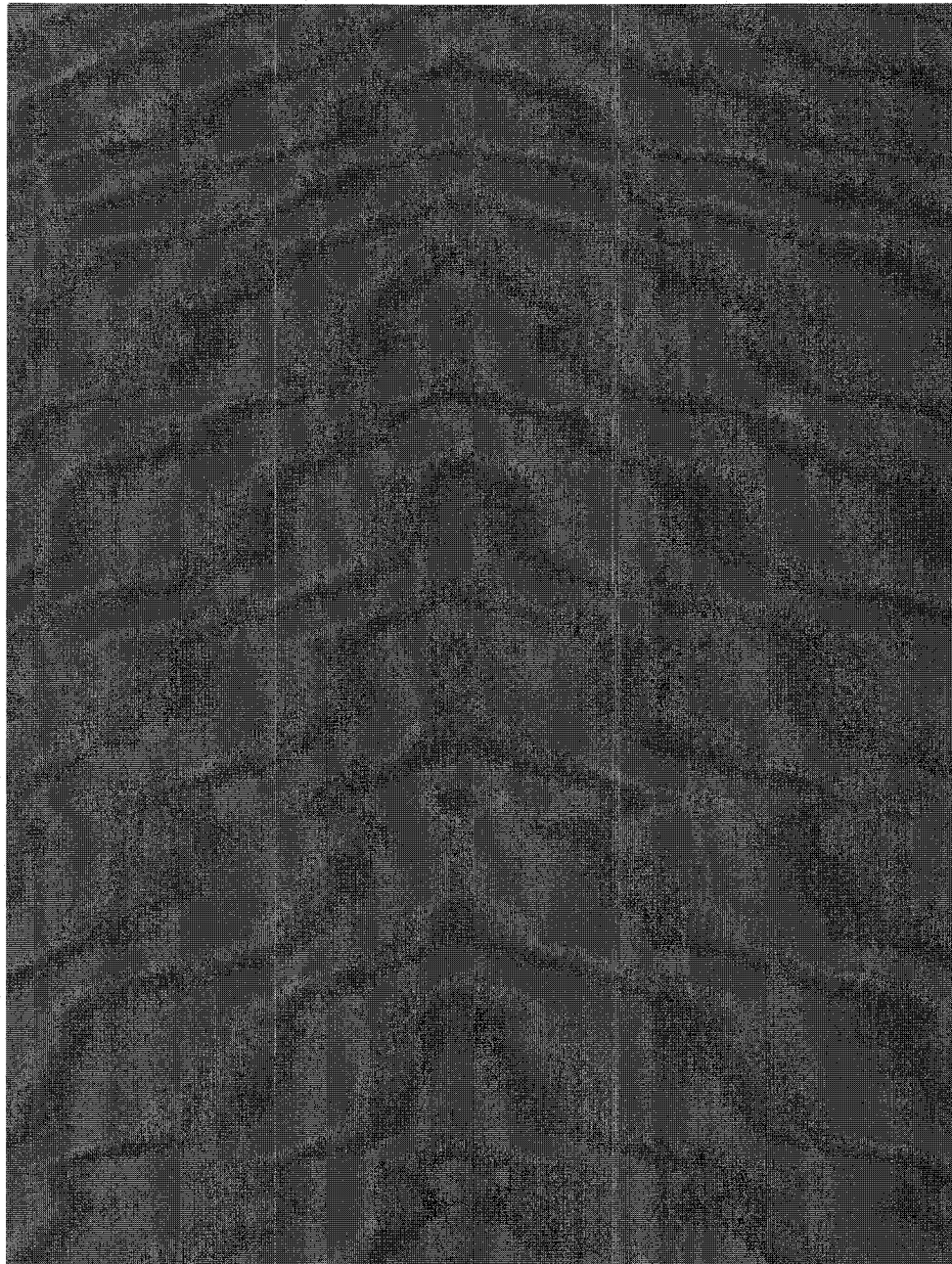
1. The location known as [REDACTED] Seattle, WA [REDACTED] is identified as follows: The location is a multi-story apartment building. The front entrance faces [REDACTED] and has glass doors with a silver-colored frame. The numbers [REDACTED] are stenciled above the door. There is a set of interior doors that lead to an entry way and elevator. [REDACTED] is located on the [REDACTED] on the [REDACTED] side of the building. The apartment door is cream colored with the numbers [REDACTED] affixed on the wall next to the door.

2. The premises to be searched includes: any appurtenances to the real property that is the SUBJECT PREMISES of [REDACTED] Seattle, WA [REDACTED], and any storage units/outbuildings.

PICTURE



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



ATTACHMENT B**Information to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections, 2251 and 2252:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- 1 f. evidence of the attachment to the COMPUTER of other storage devices or
- 2 similar containers for electronic evidence;
- 3 g. evidence of counter-forensic programs (and associated data) that are
- 4 designed to eliminate data from the COMPUTER;
- 5 h. evidence of the times the COMPUTER was used;
- 6 i. passwords, encryption keys, and other access devices that may be necessary
- 7 to access the COMPUTER;
- 8 j. documentation and manuals that may be necessary to access the
- 9 COMPUTER or to conduct a forensic examination of the COMPUTER;
- 10 k. records of or information about Internet Protocol addresses used by the
- 11 COMPUTER;
- 12 l. records of or information about the COMPUTER's Internet activity,
- 13 including firewall logs, caches, browser history and cookies, "bookmarked"
- 14 or "favorite" web pages, search terms that the user entered into any Internet
- 15 search engine, and records of user-typed web addresses; and
- 16 m. contextual information necessary to understand the evidence described in
- 17 this attachment.
- 18 3. Routers, modems, and network equipment used to connect computers to the
- 19 Internet.
- 20 4. Child pornography and child erotica.
- 21 5. Records, information, and items relating to violations of the statutes described
- 22 above including
- 23 a. Records, information, and items relating to the occupancy or ownership of
- 24 [REDACTED] Seattle, WA [REDACTED], including utility and
- 25 telephone bills, mail envelopes, or addressed correspondence; Records,
- 26 information, and items relating to the ownership or use of computer
- 27 equipment found in the above residence, including sales receipts, bills for
- 28 Internet access, and handwritten notes;

- 1 b. Records and information relating to the identity or location of the persons
- 2 suspected of violating the statutes described above; and
- 3 c. Records and information relating to sexual exploitation of children,
- 4 including correspondence and communications between users of Website
- 5 A.
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28